21. Januar 2027 · 9:00 –17:00 Uhr
Online-Veranstaltung

AKADEMIE HEIDELBERG

DORA Spezial: Informationssicherheit und IKT-Risikomanagement





Banken-Praxis-Seminar · 8 CPE-Punkte

- **Erfahrungsbericht aus einer BaFin-Prüfung mit Fokus Informationssicherheit und IKT-Risikomanagement**
- **DORA von der Informationssicherheit zu IKT-Risikomanagement**
- **Neue Pflichten des CISO, Einführung der IKT-Risikokontrollfunktion**
- **Erweiterte DORA- und TPRM-Anforderungen an die Nutzung von IKT-Dienstleistern und Cloud-Services**
- **Anforderungen an die Informationssicherheit und das IKT-Risikomanagement beim Einsatz von Künstlicher Intelligenz (KI)**

Referenten



Mike Bona-Stecki
Leiter Informationssicherheit und Business Continuity Management, stv. DOR-Beauftragter
DekaBank Deutsche Girozentrale, Frankfurt/Main



Stephan Wirth, CISSP, CISA, CRISC, CGEIT
Informationssicherheits- und Datenschutzbeauftragter
NRW.BANK, Düsseldorf

Programm

Stephan Wirth, NRW.BANK · 9:00 –10:30 Uhr

Verschärfte Anforderungen aus DORA: Informationssicherheit und Informationsrisikomanagement im Spannungsfeld zwischen Regulatorik und Praxis

- DOR-Strategie und IKT-Risikomanagementrahmen: Implementierung einer wirksamen IKT-Governance
- Etablierung eines angemessenen IKT-Risikomanagements: IKT-Risiken und Cyber-Risiken stärker im Fokus
- Akzentverschiebung durch DORA: Einführung einer IKT-Risikokontrollfunktion
- Herausforderungen IKT-Drittparteienrisikomanagement und Praxishinweise zur Maßnahmenumsetzung
- Operative IKT-Sicherheit: Anforderungen, Umsetzungsstand und (weiterhin) bestehende Schwachstellen
- Verschärfte Anforderungen an die Datenqualität
- Konkrete Anforderungen an IKT-Projekte und IT-Inventare, IDV, Berechtigungsmanagement und Schutzbedarf

Mike Bona-Stecki, DekaBank · 10:45 –12:15 Uhr

Mithilfe der Strukturanalyse und Schutzbedarfsfeststellung (Kritikalitätsanalyse) zum Sollmaßnahmenkatalog und einem höheren Informationssicherheitsniveau

- Ziel und Nutzen der Strukturanalyse, Schutzbedarfsfeststellung, Sollmaßnahmenkataloge und Risikoanalyse
- Gängige Standards: ISO 27.XXX-Reihe, BSI-Standards
- Erhebung des Informationsverbunds: Identifikation und Gruppierung der IT-Schutzobjekte
- Schutzbedarfsfeststellung auf Informations-/Prozessebene
- Erarbeitung des Sollmaßnahmenkatalogs auf Basis der Schutzbedarfs-/Strukturanalyse und gängigen Standards
- Welche Herausforderungen entstehen in der Praxis und wie kann man sie meistern?
- Darstellung der Rollen und Zuständigkeiten
- Bewertung von Soll-Ist-Abweichungen

Stephan Wirth, NRW.BANK · 13:15 –14:45 Uhr

Neue Pflichten der IKT-Risikokontrollfunktion; Abstimmung mit anderen Bereichen, Funktionen und Beauftragten

- Konkretisierung der Verantwortlichkeiten und der Aufgabenbereiche – neue Rechte und Pflichten – inwieweit ist die IKT-Risikokontrollfunktion auslagerbar?
- Wie unterstützen ISB und Risikokontrollfunktion bei der Erstellung von Strategien, Leitlinien und Prozessen zur Erreichung einer angemessenen DORA-Compliance?
- Unterstützung der Fachbereiche bei der DORA-Umsetzung
- Ermittlung von IKT-Risiken und Auswirkungsanalyse
- Best Practices und Standards für ein praxisnahes und effektives IKT-Risikomanagement
- Management von Informationssicherheitsvorfällen: Bewertung, Auswirkungsanalyse und Veranlassung angemessener Nachsorgemaßnahmen; verschärfte DORA-Meldepflichten

Mike Bona-Stecki, DekaBank · 15:00 –17:00 Uhr

Erweiterte Anforderungen an IKT-Dienstleistungen (DORA, MaRisk, EBA-GLs, AI-Act) & Cyber-Security aus dem Blickwinkel von Informationssicherheit und IKT-Risikomanagement

- Neue Abgrenzung MaRisk – DORA – EBA-GLs
- Umgang mit Cyberrisken bei Auslagerungen; Verzahnung mit dem Non Financial Risk-Management (NFR)
- Beurteilung von IKT- und Informationssicherheits-Risiken im Rahmen des Auslagerungsprozesses
- Umgang mit besonderen Herausforderungen und Risiken bei dem Bezug und der Nutzung von Cloud-Services
- Anforderungen an die vertraglichen Regelungen zur IKT-Risikomanagement bei Auslagerungen
- Business Continuity Management im Kontext von Auslagerungen und IKT-Dienstleistungen – Aufrechterhaltung der Kontinuität und Qualität der Geschäftstätigkeiten
- Umsetzungshinweise und Praxistipps

Seminarziel

Gestiegene IKT-(Dienstleister-)Risiken, Cyber-Angriffe und Lücken in der Informationssicherheit führen zunehmend häufiger zu Ausfällen kritischer und wesentlicher Geschäftsprozesse bei Banken und deren Dienstleistern. Insbesondere Angriffe von außen haben sich hierbei zu einer immanenten Bedrohung entwickelt.

Die Aufsicht erwartet unter DORA aufgrund der aktuellen geopolitischen Lage und stark erhöhter Cyber-Risiken zusätzliche (Sicherheits-)Maßnahmen der Institute. Damit einher gehen somit auch die erweiterten Aufgaben und Verantwortlichkeiten der IKT-Risikokontrollfunktion und anderer Funktionen und Beauftragter im Bereich IKT-Risikomanagement.

Auch Cloud-Dienstleistungen sind aus dem Blickwinkel der Informations-sicherheit zu beurteilen – doch wie lassen sich die mit dieser IKT-Dienstleistung verbundenen Risiken messen, beurteilen und steuern? Ziel muss es in jedem Fall sein, mithilfe der Strukturanalyse und Schutzbedarfs-feststellung zu einem aussagekräftigen Sollmaßnahmenkatalog zu gelangen und ein höheres Informations-sicherheitsniveau zu erreichen.

Das Seminar gibt wertvolle Praxistipps zur Herangehensweise und Umsetzung der aktuellen Anforderungen.

Zielgruppe

Aus der Praxis für die Praxis!
Wir wenden uns insbesondere an die Mitarbeitenden der Bereiche:

- DORA-Umsetzung, IT und Organisation, Datenschutz und Data Governance
- Informationssicherheit (ISM) und Informationsrisikomanagement (IRM)
- Notfallmanagement und Business Continuity Management (BCM/ITSCM)
- Interne Revision und IT-Revision, IT-Compliance und IT-Governance
- (Zentrales) Auslagerungsmanagement und IKT-Dienstleistersteuerung

Sowie andere interessierte Fach- bzw. Grundsatzbereiche, Vorstandsmitglieder und Geschäftsleitung sowie externe (IT-)Prüfer*innen und (IKT-)Dienstleister.

Unsere Referenten



Mike Bona-Stecki
Leiter Informationssicherheit und Business Continuity Management
stv. DOR-Beauftragter, DekaBank Deutsche Girozentrale*, Frankfurt/Main

Mike Bona-Stecki ist seit 2018 als Leiter Informationssicherheit und Business Continuity Management bei der DekaBank Deutsche Girozentrale für das Informationssicherheits-, IT-Risiko- und Business Continuity Management verantwortlich. Er leitet ein Team von Sicherheitsexperten und beschäftigt sich schwerpunktmäßig mit der Umsetzung der aufsichtsrechtlichen Anforderungen an das IT-/Informationssicherheits- und Business Continuity Management.



Stephan Wirth, CISSP, CISA, CRISC, CGEIT
Informationssicherheits- und Datenschutzbeauftragter
NRW.BANK*, Düsseldorf

Seit über zwanzig Jahren ist Herr Wirth in den Bereichen Informationssicherheit, Datenschutz und Notfallplanung in verantwortlicher Position tätig. Bei der NRW.BANK hat er seit 2018 die Funktionen des Informationssicherheits- und des Datenschutzbeauftragten inne. Die Etablierung angemessener Prozesse und Verfahren zur nachhaltigen Sicherstellung der Einhaltung der aufsichtsrechtlichen Anforderungen gehört dabei zu seinen Hauptaufgaben.

**Die Referenten geben ausschließlich ihre persönliche Auffassung und nicht notwendigerweise die eines bestimmten Instituts, der Deutschen Bundesbank, der BaFin oder einer anderen Aufsichtsbehörde wieder. Die Referenten nehmen auch keine offizielle aufsichtliche Auslegung regulatorischer Sachverhalte vor.*

Exit-Management nach DORA
26. November 2026, Online-Veranstaltung

Zertifizierter KI-Governance-Officer (CAIGO)
7. bis 9. Dezember 2026, Online-Veranstaltung

DORA-JAHRESRÜCKBLICK 2026!
10. Dezember 2026, Online-Veranstaltung

IKT Spezial: Identity & Access Management (IAM)
15. Dezember 2026, Online-Veranstaltung

Drittparteienrisikomanagement in der Praxis
18. Januar 2027, Online-Veranstaltung

Überprüfung der DORA-Konformität von (IKT-)Dienstleistern und Cloud Service Providern
19. Januar 2027, Online-Veranstaltung

Neue DORA- und Aufsichts-Anforderungen an (IKT-) Notfallmanagement & BCM
15. Januar 2027, Online-Veranstaltung

DORA-konformes IKT-Risikomanagement
3./4. Februar 2027, Online-Veranstaltung

▶ Diese und weitere Seminar-Angebote finden Sie bei uns online unter *www.akademie-heidelberg.de/online-seminare*

Zusätzliche Informationen

Fragen zu diesen Schulungen oder unserem gesamten Seminar-Programm beantworte ich Ihnen sehr gerne.



Björn Wehling
Telefon 06221/65033-44
b.wehling@akademie-heidelberg.de

Anmeldeformular

DORA Spezial: Informationssicherheit und IKT-Risikomanagement

Name

Vorname

Position

Firma

Straße / Nr.

PLZ / Ort

Telefon

E-Mail

Name der Assistenz

Datum / Unterschrift

Senden Sie Ihre Anmeldung bitte an: **anmeldung@akademie-heidelberg.de**

Termin und Seminarzeiten

Donnerstag, 21. Januar 2027
9:00–17:00 Uhr
Online-Zugang ab 8:45 Uhr

Seminar-Nr. 27 01 BA011 W

Teilnahmegebühr

€ 780,– (zzgl. gesetzl. USt)

Die Gebühr beinhaltet die Teilnahme am Online-Seminar sowie die Präsentation als PDF-Datei.
Im Anschluss an das Seminar erhalten Sie ein Zertifikat, das Ihnen die Teilnahme an der Fortbildung bestätigt.

Allgemeine Geschäftsbedingungen

Es gelten unsere Allgemeinen Geschäftsbedingungen (Stand: 01.01.2010), die wir Ihnen auf Wunsch gerne zusenden. Diese können Sie jederzeit auch auf unserer Website einsehen: www.akademie-heidelberg.de/agb

Zum Ablauf

- Vor dem Seminartag erhalten Sie von uns eine E-Mail mit einem Link, über den Sie sich direkt in die Online-Veranstaltung einwählen können.
- Für Ihre Teilnahme ist es nicht notwendig, ein Programm herunterzuladen. Sie können am Seminar direkt per *Zoom* im Browser teilnehmen.
- Über Ihr Mikrofon und Ihre Kamera können Sie jederzeit Fragen stellen und mit den Referierenden und weiteren Teilnehmenden diskutieren. Alternativ steht auch ein Chat zur Verfügung.

Druckprodukte
CO2e-bilanziert & ausgeglichen

10.26 / 27 01 BA011

AKADEMIE HEIDELBERG

AH Akademie für Fortbildung Heidelberg GmbH
Maaßstraße 32/1 · 69123 Heidelberg
Telefon 06221/65033-0
info@akademie-heidelberg.de
www.akademie-heidelberg.de